(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 20 744 A 1**

(51) Int. Cl.[7]: G 07 C 11/00

(21) Aktenzeichen: 199 20 744.5
(22) Anmeldetag: 5. 5. 1999
(43) Offenlegungstag: 16. 11. 2000

DE 199 20 744 A 1

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Jost, Hildegard, Dipl.-Math., 81667 München, DE;
Mittelmeier, Manfred, 82008 Unterhaching, DE

(56) Entgegenhaltungen:

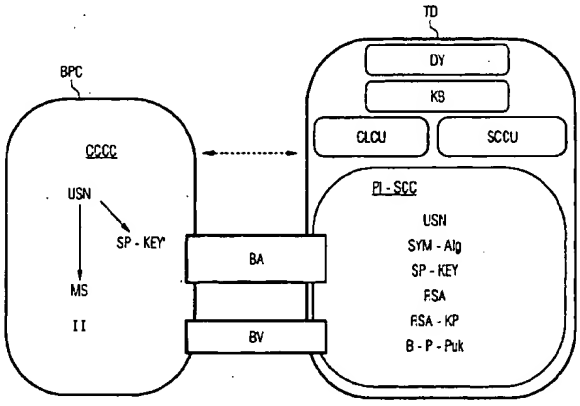
DE	198 09 574 A1
DE	43 41 880 A1
US	50 14 312
EP	08 89 448 A2
WO	99 22 341 A1
WO	98 52 162 A2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Sicherung der Echtheit von Produkten

(57) Es wird ein Konzept zur zweifelsfreien Erkennung der Echtheit von Markenprodukten vorgeschlagen, umfassend ein Verfahren zur Personalisierung eines Speicherchips für ein Markenschutz-System, ein Testgerät zum Testen von Speicherchips und zur Verifizierung der Produktdaten für ein Markenschutz-System und ein Verfahren zur Prüfung von Produktdaten. Gemäß dem vorliegenden Konzept wird jedem Markenpartikel ein Produktchip mit einer systemweit eindeutigen Signatur zugeordnet, wobei mittels eines Testgeräts eine sichere Erkennung von Markenartikeln und damit auch von Fälschungen sichergestellt ist.



DE 199 20 744 A 1

Beschreibung

Die vorliegende Erfindung bezieht sich auf ein Konzept zur zweifelsfreien Erkennung der Echtheit eines Markenprodukts. Das impliziert die Entdeckung von Fälschungen.

Der Anmeldungsgegenstand betrifft ein Verfahren zur Personalisierung eines Speicherchips für ein Markenschutz-System, ein Testgerät zum Testen von Speicherchips für ein Markenschutz-System und ein Verfahren zur Prüfung von Produktdaten.

Zur Sicherung der Echtheit von Produkten wurden bisher Merkmale an das Produkt angebracht, die die originale Urheberschaft bezeugen sollen. Dazu zählen z. B. Hologramme, Firmenlogos, die z. B. in das Produkt eingenäht werden, u. ä. Letzten Endes jedoch sind alle diese Merkmale auch fälschbar und werden von den Fälschern ebenfalls imitiert.

Aus der DE 43 41 880 A1 ist es bekannt, Halbleiterchips zum Schutz von Markenprodukten zu verwenden.

Ein Testgerät ist aus der spanischen Patentanmeldung Loureiro Benimeli, Fermin Jaime "LOUCARD – Universelles Datenkommunikationssystem für Datenträgerplatinen wie Kreditkarten oder Ähnlichen" bekannt.

Der Erfindung liegt das Problem zugrunde, Verfahren und Anordnungen anzugeben, die unter Verwendung von Produktchip und Testgerät eine optimierte Erkennung von Markenartikeln und damit auch eine sichere Erkennung von Fälschungen sicherstellen.

Das Problem wird gemäß der vorliegenden Erfindung durch die Ansprüche 1, 2 oder 4 gelöst.

Die vorliegende Erfindung stellt Verfahren bereit, die unter Verwendung von Produktchip und Testgerät eine sichere Erkennung von Markenartikeln und damit auch von Fälschungen sicherstellen.

Die Erfindung stellt eine spezielle Kombination und Anwendung von kryptographischen Verfahren bei der Erkennung von Markenprodukten bereit. Die Kombination von symmetrischer und asymmetrischer Authentisierung bei der Prüfung des Produktchips unter Einbeziehung der systemweit eindeutigen Chipnummer bietet ein höchstes Maß an Sicherheit. Die Authentisierung mit dem symmetrischen Schlüssel SP-Key garantiert die Zugehörigkeit des Chips zur Markenschutz-System, die signierte Produktinformation garantiert die Originalität des Produkts, die Einbeziehung der Chipnummer in die kryptographischen Funktionen garantiert, daß die Produktinformation nicht kopiert wurde. Jeder Produktchip enthält eine systemweit eindeutige Signatur, die nur zu diesem Produkt und nur zu diesem Produktchip paßt.

Im vorliegenden Verfahren ist die Kennzeichnung, die an das Produkt angebracht wird, nicht mehr fälschbar, weil seine Herstellung die Kenntnis von geheimen kryptographischen Schlüsseln voraussetzt. Diese Schlüssel sind jedoch nur in den Händen der autorisierten Instanzen:

- dem Systembetreiber SPB ("System Provider Brand") und
- dem Markenhersteller BNM ("Brand Name manufacturer").

Die Erfindung wird im folgenden als Ausführungsbeispiel in einem zum Verständnis erforderlichen Umfang anhand von Figuren näher erläutert. Dabei zeigen:

Fig. 1 Komponenten des Markenschutz-Systems und

Fig. 2 die Hierarchie der Schlüssel in dem Markenschutz-System.

In den Figuren bezeichnen gleiche Bezeichnungen gleiche Elemente.

Das vorliegende, erfindungsgemäße Konzept zur zweifelsfreien Erkennung der Echtheit eines Markenprodukts umfaßt

- den Enstehungs- bzw. Personalisierungsweg des Produktchip
- die Personalisierung von Testgeräten und Schlüsselkarten
- den Ablauf der Produktprüfung
- den Test von Testgeräten
- die Schlüsselhierarchie des Systems (Zertifizierungshierarchie)
- die Verteilung der einzelnen Schlüssel auf die Komponenten
- die Abläufe des Schlüsselupdates.

Soweit im Zusammenhang mit der vorliegenden Erfindung von Brand gesprochen wird, wird darunter ein bestimmtes System zum Schutz von Marken-Produkten vor unerlaubter Nachahmung verstanden.

1.1 Der Produktchip

Der Produktchip BPC (für: Brand Product Chip) weist auf:

- einen intelligenten, kontaktlosen Speicherchip, dessen Lese- und Schreibzugriffe durch kryptographische Challenge-Response und Verschlüsselungs-Verfahren geschützt werden. Dazu enthält der Chip einen
- symmetrischen kryptographischen Algorithmus SYM-Alg
- sowie mindestens einen geheimen chipspezifischen Schlüssel SP-key' zu diesem Algorithmus.
- eine eindeutige Identifikationsnummer USN (für: unique serial number). Der chipspezifische Schlüssel ist dem Product Chip mit dieser Identifikationsnummer eindeutig zugeordnet und nach dem üblichen Verfahren der Erzeugung von abgeleiteten Schlüsseln aus einem Masterschlüssel und einer eindeutigen Identifikationsnummer abgeleitet.
- Darüber hinaus enthält der Product Chip Informationen über das Produkt, z. B. Markenname, Produktname, Ort und Zeit der Produktion.

Diese Produktinformationen enthalten auch eine digitale Signatur, die vom Markenhersteller mit einem asymmetrischen kryptographischen Algorithmus ASYM-Alg unter Verwendung des privaten Schlüssels B-P-PrK des Markenherstellers erzeugt wurde. Die Signatur schließt neben den Produktinformationen auch die eindeutige Chipnummer mit ein, um Kopierversuche der signierten Produktdaten nutzlos zu machen. Jeder Produktchip enthält also damit eine systemweit eindeutige Signatur, die nur zu diesem Produkt und nur zu diesem Produktchip paßt. Ein Produktchip BPC weist also ein für seine Chipnummer erstelltes Zertifikat auf.

1.1.2 Das Testgerät

Das Testgerät enthält:

- Eine Anzeigeeinrichtung DY (für: Display)
- eine Eingabeeinrichtung KB (für: Keyboard)
- eine Einheit CLCU (für: Contactless Communication Unit) für die kontaktlose Kommunikation mit dem Produktchip,
- eine Chipkartenkontaktiereinheit SCCU (für: Smart Card Contacting Unit) für die kontaktbehaftete oder

kontaktlose Kommunikation mit Schlüsselkarten (zum Laden von neuen Schlüsseln) und
- einen Smart-Card-Prozessorchip PI-SCC (für: Plug-In-Smart Card Chip) mit kryptographischem Coprozessor. Im Smart-Card-Chip des Testgeräts laufen der symmetrische Algorithmus SYM-Alg und der asymmetrische Algorithmus ASYM-Alg z. B. RSA (Rivest, Shamir, Adleman).
- Der Smart-Card-Chip des Testgeräts enthält
- eine systemweit eindeutige Seriennummer USN (für: unique serial number),
- den globalen SYM-Alg-Schlüssel SP-KEY des Systembetreibers
- ein individuelles asymmetrisches Schlüsselpaar (TD-PrK, TD-PuK) mit Public-Key-Zertifikat,
- ein Public-Key-Zertifikat des Schlüssels (SP-P-PrK, SP-P-PuK), das den öffentlichen Schlüssel des Schlüsselpaars (TD-PrK, TD-PuK) als zu dieser eindeutigen Seriennummer gehörig zertifiziert,
- die Public-Key-Zertifikate der Markenhersteller (Brand-Pers-Puk-Cert), zertifiziert vom Systembetreiber mit dessen Root-Schlüssel.
- das Public-Key-Zertifikat des öffentlichen Root-Schlüssels des Systembetreibers (SP-Root-PuK-Cert), mit dem die Public-Keys der Markenhersteller und die Personalisierungszertifikate SP-P-PuK-Cert verifizierbar sind (inklusive Vorgänger-Generation).

In einer besonderen Ausgestaltung fallen der Rootschlüssel des Systembetreibers SP-Root-PA nebst dem Public-Key-Zertifikat (SP-Root-PuK-Cert) des öffentlichen Root-Schlüssels des Systembetreibers und das Schlüsselpaar aus öffentlichem und privatem Schlüssel SP-P-PA nebst dem Personalisierungs-Zertifikat SP-P-PuK-Cert des Systembetreibers zusammen.

Das Testgerät weist also ein individuell für seine Seriennummer erstelltes Zertifikat auf.

1.1.3 Die Personalisierungsmaschine

Die Personalisierungsmaschine ermöglicht es dem Markenhersteller, seine signierten Produktinformationen in den Chip zu schreiben. Diese Maschine wird integriert in den Produktionsablauf. Sie enthält

- den Schlüssel des Systembetreibers SP-KEY, mit dessen Hilfe die zu verarbeitenden Chips als echte Brand-Chips authentisiert werden können (optional),
- das Schlüsselpaar (Brand-Pers-PrK, Brand-Pers-PuK), mit dessen Hilfe die Produktdaten für den Produktchip signiert werden.

1.1.4 Die Schlüsselkarte

Die Schlüsselkarte KC (für: Key Card) ist als Prozessorchipkarte mit kryptographischem Coprozessor für asymmetrische Kryptographie ausgebildet. Sie ist kontaktbehaftet oder kontaktlos ausgebildet und wirkt mit der Chipkartenkontaktiereinheit SCCU oder mit der Einheit für kontaktlose Kommunikation CLCU des Testgerätes zusammen. Sie enthält wie das Testgerät

- eine systemweit eindeutige Seriennummer USN sowie
- ein individuelles asymmetrisches Schlüsselpaar (KC-PrK, KC-PuK) mit Public-Key-Zertifikat,
- ein Public-Key-Zertifikat des Schlüssels (SP-P-PrK, SP-P-PuK), das den öffentlichen Schlüssel des Schlüsselpaars (KC-PrK, KC-PuK) als zu dieser eindeutigen Seriennummer gehörig zertifiziert.
- das Public-Key-Zertifikat des öffentlichen Root-Schlüssels des Systembetreibers (SP-Root-PuK-Cert), mit dem die Personalisierungszertifikate SP-P-PuK-Cert verifiziert werden können (inklusive Vorgänger-Generation).

Die Schlüsselkarte ist das Transportmedium für die Verteilung der Public Key-Zertifikate der Markenhersteller und des Brand-Root-Zertifikats in alle Testgeräte sowie für den Update des geheimen symmetrischen Schlüssels SP-Key in den Testgeräten.

1.2 Die Instanzen und ihre Verantwortlichkeiten

Folgende Instanzen sind in das System involviert:

1.2.1 Der Systembetreiber SPB

Der Systembetreiber hat folgende Aufgaben:

- er stellt den anderen Instanzen alle benötigten Hard- und Softwarekomponenten zur Verfügung:
  - die Brand-Chips
  - die Personalisierungsmaschine
  - die Testgeräte
  - die Schlüsselkarten
- er erzeugt, verwaltet und verteilt den geheimen symmetrischen Systemschlüssel SP-KEY,
- er beauftragt den Brand-Chip-Personalisierer, den Testgerät-Personalisierer und den Schlüsselkartenpersonalisierer mit der Personalisierung der jeweiligen Komponenten vor Auslieferung mit den entsprechenden kryptographischen Schlüsseln,
- er unterhält ein Trust Center, in dem die öffentlichen Schlüssel der Brand-Personalisierungsschlüsselpaare und die öffentlichen Schlüssel der Markenhersteller zertifiziert werden.

1.2.2 Der Brand-Chip-Personalisierer

Er bekommt vom Systembetreiber (bzw. dessen Trust Center) den geheimen Systemschlüssel SP-KEY und personalisiert damit die Brand-Chips (siehe auch Kapitel 1.3.1 Personalisierung des Brand-Chips). Er ist für die Geheimhaltung des Schlüssels SP-KEY verantwortlich.

1.2.3 Der Brand-Testgerät-Personalisierer

Er bekommt vom Systembetreiber (bzw. dessen Trust Center) den geheimen Systemschlüssel SP-KEY und personalisiert damit die Smart-Card-Chips der Testgeräte (siehe auch Kapitel 1.3.3 Personalisierung des Testgerät-Smart-Card-Chips). Dazu muß er sich auch ein Personalisierungsschlüsselpaar erzeugen, dessen öffentlicher Schlüssel vom Trust Center des Systembetreibers zertifiziert wird. Mit dem privaten Schlüssel dieses Schlüsselpaars signiert er die öffentlichen Schlüssel der Testgeräte, die er personalisiert. Er ist für die Geheimhaltung des Schlüssels SP-KEY und seines privaten Personalisierungsschlüssels verantwortlich.

1.2.4 Der Brand-Schlüsselkarten-Personalisierer

Er erzeugt sich ein Personalisierungsschlüsselpaar, dessen öffentlicher Schlüssel vom Trust Center des Systembe-

treibers zertifiziert wird. Mit dem privaten Schlüssel dieses Schlüsselpaars signiert er die öffentlichen Schlüssel der Schlüsselkarten, die er personalisiert. (siehe Kapitel 1.3.4 Personalisierung der Schlüsselkarten).

Er ist für die Geheimhaltung seines privaten Personalisierungsschlüssels verantwortlich.

1.2.5 Der Markenhersteller

Der Markenhersteller ist gegenüber dem Systembetreiber für die Geheimhaltung des SP-KEY verantwortlich. Der Markenhersteller

- erzeugt sein asymmetrisches Schlüsselpaar, läßt den öffentlichen Schlüssel vom Systembetreiber zertifizieren und ist für die sichere Speicherung seines privaten Schlüssels verantwortlich.
- verteilt sein Public-Key-Zertifikat an alle Händler, Großhändler und Fahnder.
- bekommt vom Systembetreiber die mit SP-KEY' personalisierten Chips.
- bringt den Chip an seinem Markenprodukt an,
- liest die Chip-Seriennummer,
- prüft ob es ein echter Brand-Chip ist (durch eine Authentisierung mit SK-KEY) und
- signiert seine Produktinformation für diesen Chip (unter Einbeziehung der Chipnummer) mit seinem privaten Schlüssel und schreibt diese signierte Produktinformation in den Chip.

1.2.6 Der Händler/Großhändler

- er muß die ihm gelieferten Markenprodukte mit seinem Testgerät prüfen (siehe Kapitel 1.3.5 Ablauf der Produktprüfung)
- optional kann die Verkaufstransaktion im Product Chip vermerkt werden. Dadurch wird der Product Chip entwertet und eine Wiederverwendung an einem anderen (gefälschten) Produkt unmöglich gemacht.
- Update des symmetrischen Schlüssels SP-KEY sowie aller benötigten Public-Key-Zertifikate in seinem Testgerät und in den Testgeräten seiner Kunden durch Schlüsselladen von der speziellen Schlüsselkarte.

1.2.7 Der Fahnder

- er prüft Waren beim
Händler/Großhändler,
beim Zoll.
...
mit seinem Testgerät. (siehe Kapitel
- 1.3.5 Ablauf der Produktprüfung)
- er prüft Testgeräte, ob sie echte Brand-Testgeräte sind und nicht "chronische Jasager" oder anders manipulierte Testgeräte, die Fälschungen als echte Markenprodukte ausgeben.

1.2.8 Der Endverbraucher

Der Endverbraucher hat die Möglichkeit, ein Testgerät zu erwerben. Er kann sich die Public-Key-Zertifikate der Markenhersteller beim Händler in sein Testgerät laden lassen und dann die Produkte prüfen.

1.3 Abläufe

1.3.1 Personalisierung des Brand-Chips

Dieser Vorgang findet beim Brand-Chip-Personalisierer in abgesicherter Umgebung vor Auslieferung der Chips an den Markenhersteller statt. Im einzelnen sind folgende Schritte gegeben:

- Authentifikation des Produktchips mit dem Transport-Schlüssel des Chipherstellers
- Lesen der Seriennummer USN des Produktchips
- Erzeugen eines individuellen Schlüssels SP-KEY', der von dem globalen Schlüssel SP-KEY abgeleitet ist
- Einschreiben des abgeleiteten Schlüssels SP-KEY' in den Produktchip.

1.3.2 Personalisierung des Produktchips

Dieser Vorgang findet beim Markenhersteller statt vor Auslieferung der Markenware an die Händler/Großhändler. Der Sicherheits-Server des Markenherstellers hat den globalen Schlüssel SP-KEY des Systembetreibers gespeichert und erzeugt bzw. speichert den privaten Schlüssel B-P-PrK sowie den öffentlichen Schlüssel B-P-PuK des Markenherstellers.

Im einzelnen sind folgende Schritte gegeben:

- Anbringen des Produktchips am Produkt
- Lesen der Seriennummer USN des Produktchips
- Authentifikation des Produktchips als Brand-Chip durch Anwendung des globalen Schlüssels SP-KEY
- Erzeugen eines Produkt-Zertifikats für diesen Produktchip durch Anwendung des privaten Schlüssel B-P-PrK des Markenherstellers
- Einschreiben des Produkt-Zertifikats in den Produktchip.

1.3.3 Personalisierung des Testgerät-Smart-Card-Chips

Dieser Vorgang findet beim Testgerät-Personalisierer vor Auslieferung der Testgeräte in einer Umgebung, die in hohem Maße abgesichert ist, statt.

Im einzelnen sind folgende Schritte gegeben:

- Die Personalisierungs-Maschine erzeugt mit dem asymmetrischen Algorithmus ASYM-Alg, wie z. B. dem RSA Algorithmus (Rivest, Shamir, Adleman)-Algorithmus, ein neues Schlüsselpaar
- Die Personalisierungs-Maschine liest die eindeutige Identifikationsnummer ID des Testgeräts, die tatsächlich die eindeutige Identifikationsnummer ID des Smart-Card-Chips ist, und erzeugt ein Zertifikat, das den öffentlichen Schlüssel PuK des neuen Schlüsselpaares zu der eindeutigen Identifikationsnummer ID des Smart-Card-Chips bestätigt. Sie unterzeichnet das Zertifikat durch ihre aktuelle SP-P-PrK und schreibt das zertifizierte Schlüsselpaar in den Smart-Card-Chip
- Die Personalisierungs-Maschine schreibt ihr aktuelles SP-P-PuK Zertifikat in den Smart-Card-Chip
- Die Personalisierungs-Maschine schreibt den aktuellen und die vorhergehende Version des globalen Schlüssels SP-KEY in den Smart-Card-Chip
- Die Personalisierungs-Maschine schreibt den aktuellen und die vorhergehende Version des SP-Root-PuK-Certificate in den Smart-Card-Chip.

1.3.4 Personalisierung der Schlüsselkarten

Dieser Vorgang findet beim Schlüsselkarten-Personalisierer vor Auslieferung der Schlüsselkarte in einer Umgebung, die in hohem Maße abgesichert ist, statt.

Im einzelnen sind folgende Schritte gegeben:

- Die Personalisierungs-Maschine erzeugt mit dem asymmetrischen Algorithmus ASYM-Alg, wie z. B. dem RSA Algorithmus (Rivest, Shamir, Adleman)-Algorithmus, ein neues Schlüsselpaar
- Die Personalisierungs-Maschine liest die eindeutige Identifikationsnummer ID der Schlüsselkarte und erzeugt ein Zertifikat, das den öffentlichen Schlüssel PuK des neuen Schlüsselpaares zu der eindeutigen Identifikationsnummer ID der Schlüsselkarte bestätigt. Sie unterzeichnet das Zertifikat und schreibt das zertifizierte Schlüsselpaar in die Schlüsselkarte
- Die Personalisierungs-Maschine schreibt das aktuelle öffentliche Schlüssel-Zertifikat des Systembetreibers (SP-P-PuK-Cert) in die Schlüsselkarte
- Die Personalisierungs-Maschine schreibt den aktuellen und die vorhergehende Version des SP-Root-PuK-Certificate in die Schlüsselkarte.

1.3.5 Ablauf der Produktprüfung

Dieser Vorgang kann überall stattfinden: beim Händler, Großhändler, beim Endverbraucher, usw. Er kann von jedem durchgeführt werden, der im Besitz eines Testgeräts ist (Händler, Großhändler, Endverbraucher, Fahnder, usw.)

- Identifikationsnummer lesen
- Chip als echten Brand-Chip authentisieren mittels challenge-response-Verfahren mit Schlüssel SP-KEY'
- signierte Produktdaten vom Chip lesen
- Signatur unter Einbeziehung der Chipnummer mit dem öffentlichen Schlüssel des Markenherstellers verifizieren.

In einer besonderen Ausführungsform werden der Ort und das Datum von Verkaufsvorgängen in den Speicherchip BPC eingeschrieben, womit eine Entwertungs-Information gegeben ist.

1.3.6 Ablauf der Schlüsselladefunktionen

Das Update (Aktualisierung) des globalen Schlüssels SP-KEY im Testgerät läuft im einzelnen in folgenden Schritten ab:

1) Gegenseitige (mutual) Authentifikation zwischen Testgerät und Schlüsselkarte unter Verwendung ihrer durch einen asymmetrischen Algorithmus ASYM-Alg gebildeten individuellen Schlüsselpaare
   - Lesen der PuK-Zertifikate des Partners (individueller PuK und Personalisierungs-PuK) und deren Verifizierung unter Verwendung der entsprechenden SP-Root-PuK
   - Erzeugen und Senden einer Zufallszahl an den Partner
   - Verschlüsseln der empfangenen Zufallszahl mit dem eigenen privaten Schlüssel und Zurücksenden des Ergebnisses
   - Verifizieren des vom Partner erhaltenen Ergebnisses mit dessem öffentlichen Schlüssel.
2) Laden des neuen SP-KEY Master-Schlüssels von der Schlüsselkarte in das Testgerät
   - Der neue SP-KEY Master-Schlüssel, der in der Schlüsselkarte mit dem vorhergehenden SP-KEY Master-Schlüssel verschlüsselt gespeichert ist, wird in der Schlüsselkarte zusätzlich mit dem öffentlichen Schlüssel des Testgeräts TD-PuK verschlüsselt,
   - der neue SP-KEY Master-Schlüssel wird zum Testgerät gesandt
   - das Testgerät entschlüsselt den empfangenen SP-KEY mit seinem privaten Schlüssel und mit dem vorhergehenden SP-KEY Master-Schlüssel sowie speichert ihn in dem EEPROM (Electrically Erasable Programmable Read Only Memory) des Smart-Card-Chip.

Alle kryptographischen Funktionen in dem Testgerät laufen in dem Smart-Card-Chip ab. Geheime Schlüssel erscheinen niemals im Klartext in der Firmware des Testgeräts außerhalb des Smart-Card-Chips. Der Smart-Card-Chip ist ein Sicherheits-Controller, der physikalisch und logisch gegen Angriffe geschützt ist.

Das Update (Aktualisierung) des Brand Public Key Zertifikats B-P-PuK-Cert im Testgerät läuft im einzelnen in folgenden Schritten ab:

- Gegenseitige (mutual) Authentifikation zwischen Testgerät und Schlüsselkarte unter Verwendung ihrer durch einen asymmetrischen Algorithmus ASYM-Alg gebildeten individuellen Schlüsselpaare
- Laden des neuen B-P-PuK-Cert in das Testgerät im Klartext
- Verifizierung der Brand-Signatur des B-P-PuK-Cert in dem Testgerät.

Das Testgerät muß das vorhergehende Brand Public Key Zertifikat behalten solange es gültig ist oder sogar länger um abgelaufene Produkt Zertifikate zu erkennen.

Das Update (Aktualisierung) des SP-Root-PuK-Cert im Testgerät läuft im einzelnen in folgenden Schritten ab:

- Gegenseitige (mutual) Authentifikation zwischen Testgerät und Schlüsselkarte unter Verwendung ihrer durch einen asymmetrischen Algorithmus ASYM-Alg gebildeten individuellen Schlüsselpaare
- Laden des neuen SP-Root-PuK-Cert in das Testgerät im Klartext
- Verifizierung der Brand-Signatur des neuen SP-Root-PuK-Cert mit dem vorhergehenden SP-Root-PuK in dem Testgerät
- Erzeugen eines Fingerprints (Prüfsumme) des neuen SP-Root-PuK-Cert durch das Testgerät und Anzeige an den Benutzer für Überprüfungszwecke.

Das Testgerät muß das vorhergehende SP-Root-PuK-Cert behalten solange es gültig ist.

Die Schlüsselkarte muß das vorhergehende SP-Root-PuK-Cert beinhalten um ältere Testgeräte zu authentifizieren.

1.3.7 Test des Testgeräts mit einer speziellen Testkarte

Ist das Testgerät ein authentisches Brand-Gerät?

- Lesen und Anzeigen von Test-Daten von der Test-Karte. Diese Daten können erst nach erfolgreicher

ASYM-Alg-Authentifikation mit dem individuellen Schlüsselpaar gelesen werden.

Enthält das Testgerät die richtigen SP-KEY-Generationen?

- Lesen und Anzeigen von Test-Daten von der Test-Karte. Diese Daten können erst nach erfolgreicher Alg-Authentifikation mit dem SP-KEY gelesen werden.

Enthält das Testgerät die richtigen SP-Root-PuKs?

- Anzeigen der SP-Root-PuKs einschließlich ihrer Fingerabdrücke;
- Versuch ein nicht-authentisches SP-Root-PuK-Cert zu laden und Testen der Antwort
- Versuch ein authentisches SP-Root-PuK-Cert zu laden und Testen der Antwort.

Enthält das Testgerät die richtigen B-P-PuKs?

- Anzeigen der B-P-PuKs einschließlich ihrer Fingerprints;
- Verifizierung eines authentischen Produktchips und testen der Antwort
- Verifizierung eines nicht-authentischen Produktchips und testen der Antwort.

Bei dem vorliegenden Konzept werden die Produktdaten in den Produktchips BPC, die Schlüssel in den Testgeräten TD und in den Schlüsselkarten KC – wie in **Fig.** 2 verdeutlicht – hierarchisch mittelbar oder unmittelbar signiert bzw. zertifiziert.

Bezugszeichenliste

SPB Systembetreiber Markenkennzeichnungsverfahren (für: System Provider Brand)
BNM Markenhersteller (für: Brand Name Manufacturer)
BPC kontaktloser Product Chip (für: Brand Product Chip)
SYM-Alg Symmetrischer kryptographischer Algorithmus
ASYM-Alg Asymmetrischer kryptographischer Algorithmus
RSA asymmetrischer Algorithmus von Rivest, Shamir, Adleman
RSA-PA RSA-Algorithmus-Schlüsselpaar (für: RSA-Key-Pair)
SP-KEY globaler geheimer SYM-Alg Schlüssel des Systembetreibers (für: System Provider Key)
SP-KEY' individueller, chipspezifischer Schlüssel, der von dem globalen Schlüssel SP-KEY abgeleitet ist
B-P-PuK öffentlicher Schlüssel des Markenherstellers (für: Brand-Personalisation-Public Key)
B-P-PrK privater Schlüssel des Markenherstellers (für: Brand-Personalisation-Private Key)
B-P-Pa Schlüsselpaar aus öffentlicher und privatem Schlüssel des Markenherstellers (für: Brand-Personalisation-Pair)
B-P-PuK-Cert Öffentliche Schlüssel-Zertifikate der Markenhersteller (für: Brand-Personalisation-Public Key-Certificate)
TD-PuK öffentlicher Schlüssel des Testgeräts (für: Test Device-Public Key)
TD-PrK privater Schlüssel des Testgeräts (für: Test Device-Private Key),
TD-Pa Individulles, asymmetrisches Schlüsselpaar für Testgerät (für: Test Device-Pair)
SP-P-PuK (für: System Provider-Personalisation-Public Key)
SP-P-PrK (für: System Provider-Personalisation-Private Key)
SP-P-Pa Schlüsselpaar aus öffentlicher und privatem Schlüssel des Systembetreibers (für: System Provider-Personalisation-Pair)
SP-P-PuK-Cert Personalisierungs-Zertifikat des Systembetreibers (für: System Provider-Personalisation-Public Key-Certificate)
SP-Root-Pa Rootschlüssel des Systembetreibers (für: System Provider-Root-Pair)
SP-Root-PrK privater Root-Schlüssel des Systembetreibers
SP-Root-PuK-Cert Zertifikat des öffentlichen Root-Schlüssels des Systembetreibers(für: System Provider-Root-Public Key-Certificate)
KC-PuK öffentlicher Schlüssel der Schlüsselkarte.(für: Key Card-Public Key)
KC-PrK privater Schlüssel der Schlüsselkarte (für: Key Card-Private Key)
KC-Pa Individuelles, asymmetrisches Schlüsselkarten Paar aus KC-PrK, KC-PuK (für: Key Card-Pair)
BTC Zentrale des Markenkennzeichnungsverfahrens (für: Brand Trust Center)
BTD Testgerät (für: Brand Test Device)
USN systemweit eindeutige Seriennummer (für: unique serial number)
DY Anzeigeeinrichtung (für: Display)
KB Eingabeeinrichtung (für: Keyboard)
CLCU Einrichtung für die kontaktlose Kommunikation mit dem Produktchip (für: Contactless Communication Unit)
SCCU Chipkartenkontaktiereinheit für die Kommunikation mit Schlüsselkarten (für: Smart Card Contacting Unit)
PI-SCC Smart-Card-Processorchip mit kryptographischem Coprozessor (für: Plug-In-Smart Card Chip)
KC kontaktbehaftete Schlüsselkarte mit kryptographischem Coprozessor für asymmetrische Kryptographie (für: Key Card)
CCCC kontaktloser Chipkarten Chip (für: Contactless Chip Card Chip)
MS Produktdaten einschließlich Signatur (für: manufacturer's signature)
II Entwertungsinformation (für: Invalidation Information)
BA Authentifizierung als zum Markenschutzverfahren zugehörig (für: Brand Authentikation)
BV Verifikation der Markenkennzeichnung (für: Brand Verifikation)
PE Personalisierer

Patentansprüche

1. Verfahren zur Personalisierung eines Speicherchips für ein Markenschutz-System, demzufolge zur Personalisierung beim Systemprovider
   - die eindeutige Identifikationsnummer (USN) des Speicherchips gelesen wird,
   - aus einem globalen, geheimen Schlüssel (SP-KEY) und der Identifikationsnummer ein individueller Schlüssel (SP-KEY') abgeleitet wird,
   - der individuelle Schlüssel (SP-KEY') in den Speicherchip geschrieben wird,

   zur Personalisierung beim Markenhersteller
   - die eindeutige Identifikationsnummer (USN) des Speicherchips gelesen wird,
   - mit dem Private Key des Markenherstellers (B-P-PrK) eine Signatur über die Identifikationsnummer und eine Produktinformation gebildet wird,
   - die Produktinformation und die Signatur in den Speicherchip geschrieben werden.
2. Testgerät (TD) für ein Markenschutz-System um-

fassend eine Einheit (CLCU) für die kontaktlose Kommunikation mit einem Chip, umfassend
einen Smart-Card-Prozessorchip PI-SCC, der
- einen symmetrischen kryptographischen Algorithmus SYM-Alg,
- den globalen SYM-Alg-Schlüssel SP-KEY des Markenschutz-Systembetreibers,
- einen asymmetrischen kryptographischen Algorithmus ASYM-Alg,
- die Public-Key-Zertifikate (B-P-PuK-Cert) der Markenhersteller,

aufweist.

3. Testgerät (TD) für ein Markenschutz-System nach Anspruch 2 dadurch gekennzeichnet, daß der Smart-Card-Prozessorchip PI-SCC
- eine eindeutige Seriennummer,
- ein individuelles asymmetrisches Schlüsselpaar (TD-PrK, TD-PuK) mit Public-Key-Zertifikat TD-PuK-Cert signiert durch einen übergeordneten privaten Schlüssel des Systembetreibers,
- das Public-Key-Zertifikat des öffentlichen Schlüssels des Systembetreibers, der zur Verifizierung der Public-Key-Zertifikate der Markenhersteller benutzt wird, aufweist.

4. Verfahren zur Prüfung von Produktdaten in einer Anordnung, in der
- ein Testgerät (TD) mit einem Produktchip (BPC) in Wirkverbindung steht,
- das Testgerät
  - einen symmetrischen Algorithmus (SYM-Alg),
  - einen asymmetrischen Algorithmus (ASYM-Alg),
  - einen globalen symmetrischen Schlüssel (SP-KEY)
  - die Public-Key-Zertifikate (B-P-PuK-Cert) der Markenhersteller,

  aufweist
- der Produktchip einen symmetrischen Algorithmus (SYM-Alg), eine eindeutige Identifikationsnummer(USN) sowie einen aus dem globalen Schlüssel (SP-KEY) und der Identifikationsnummer (USN) abgeleiteten, individuellen Schlüssel (SP-KEY') aufweist,

demzufolge eine Authentifizierung des Chips und Verifizierung der Produktdaten gegeben sind derart daß,
- das Testgerät die Identifikationsnummer (USN) aus dem Produktchip liest,
- aus dieser Identifikationsnummer und dem globalen Schlüssel SP-KEY der chipspezifische Schlüssel SP-KEY' ableitet wird
- mit dem Schlüssel SP-KEY' der Produktchip durch ein Challenge-Response-Verfahren authentifiziert wird
- nach erfolgreicher Authentifizierung des Produktchips das Testgerät die Produktinformationen und die Signatur aus dem Produktchip liest, wobei die mit dem Private Key des Markenherstellers (B-P-PrK) erzeugte Signatur über die Identifikationsnummer und die Produktinformation gebildet ist
- das Testgerät diese Signatur mit dem Public Key des Markenherstellers (B-P-PuK) verifiziert und so die Echtheit der Produktinformationen und ihre Zugehörigkeit zu diesem Chip verifiziert.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 199 20 744 A1
Int. Cl.[7]: G 07 C 11/00
Offenlegungstag: 16. November 2000

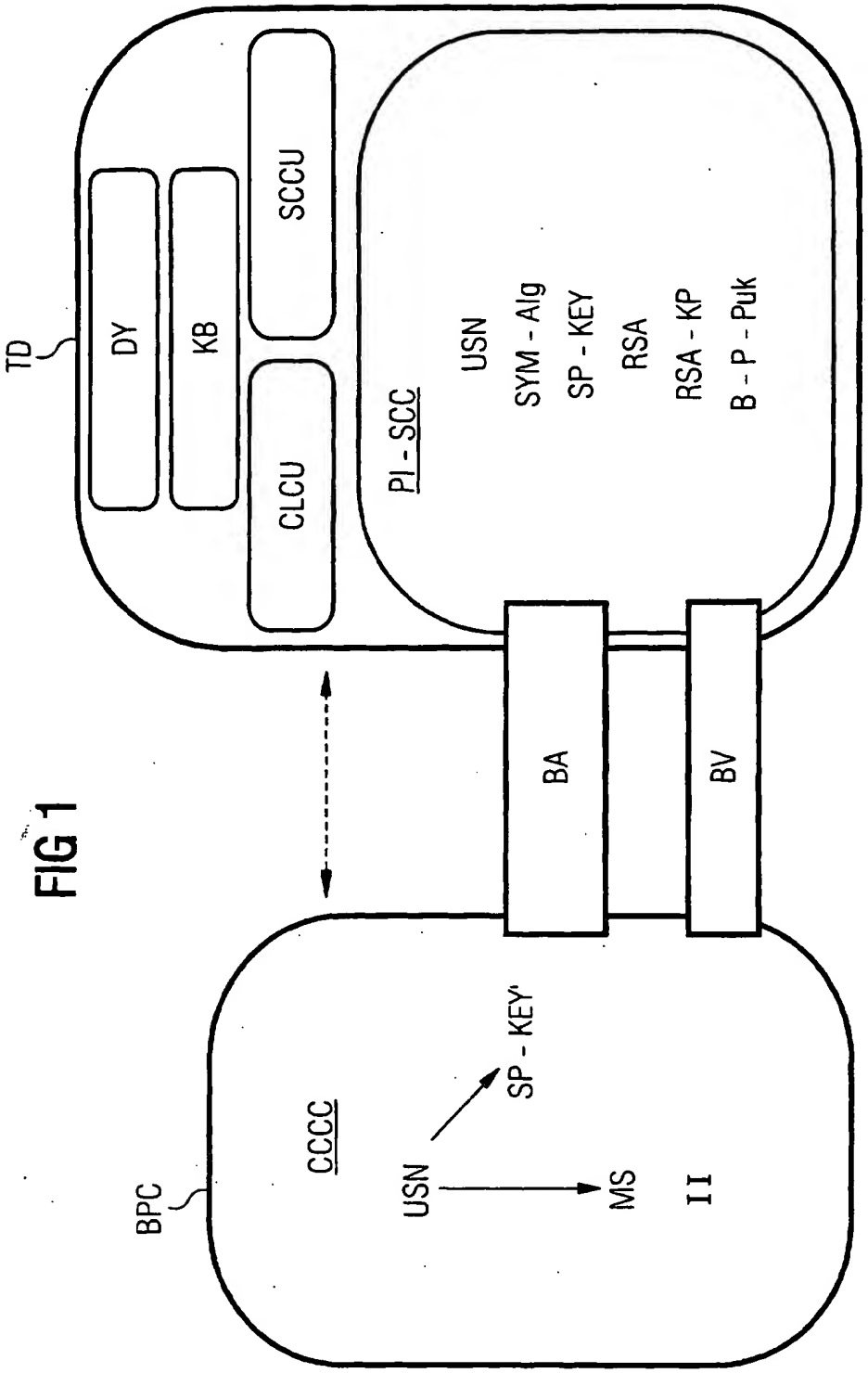


FIG 1

Nummer: DE 199 20 744 A1
Int. Cl.[7]: G 07 C 11/00
Offenlegungstag: 16. November 2000

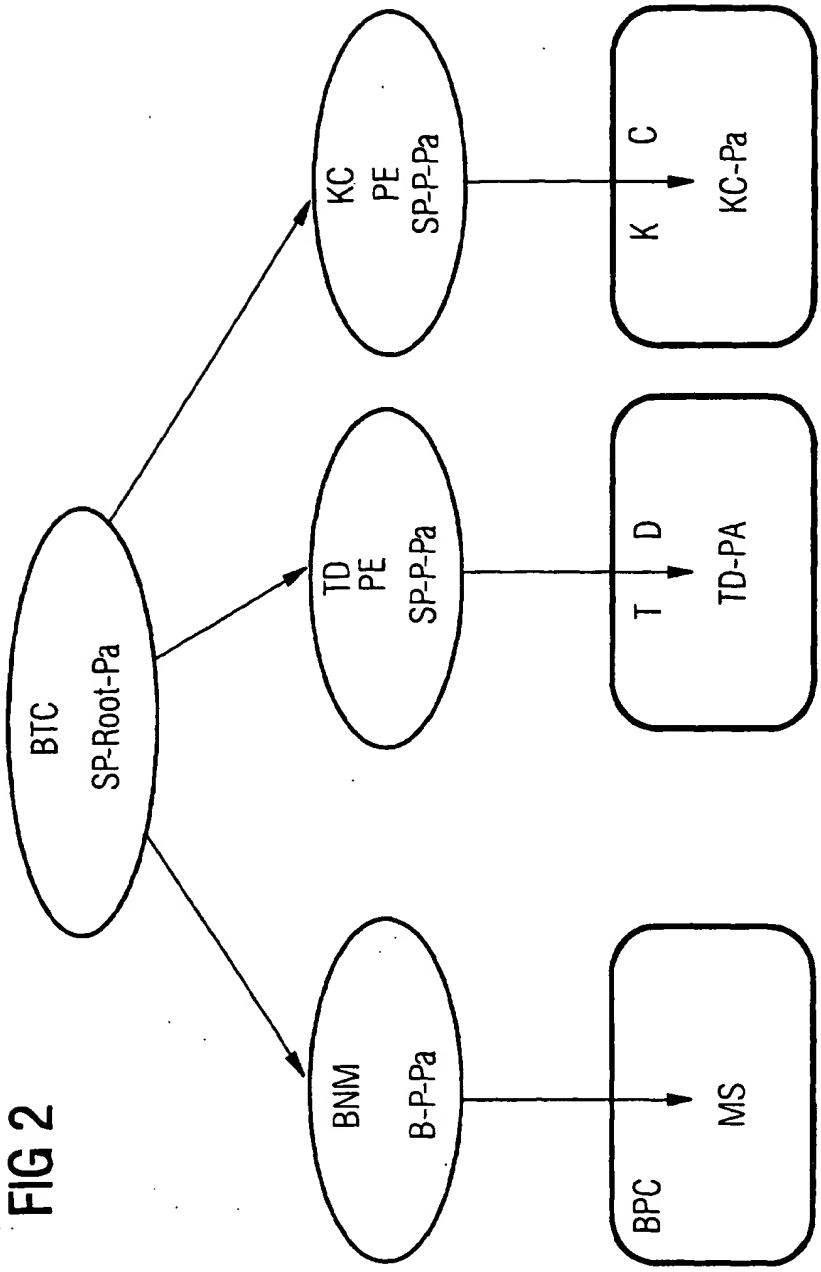


FIG 2